UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,242	06/26/2001	Zheng Qi	BRCMP013C	3440

22434	7590	01/27/2005

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO 90C (Rev 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/892,242	QI ET AL.
	Examiner	**Art Unit**	
	Ponnoreay Pich	2135	

-- *The MAILING DATE of this communication appears on th cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is·
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08),
Paper No(s)/Mail Date 2/14/02, 10/6/03, and 11/8/04

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claims 1-37 have been examined and are pending.

Information Disclosure Statement

The examiner has considered the IDS submitted by the applicant.

Specification

The disclosure is objected to because of the following informalities:

1. On page 5, line 14, the applicant discuss Figure 4. Figure 4 does not exist
   among the drawings submitted by the applicant. Figure 4A and 4B do exist.
   The applicant may want to consider updating the description in the
   specification on page 5 to make this clearer.

2. On page 13, the first sentence of the third paragraph states: "As will be
   appreciated by one of skill the art, various control signals." This sentence
   appears to be incomplete and the examiner wishes to draw the applicant's
   attention to it.

3. On page 21, last paragraph, the applicant talks about a "prorogation stage".
   The examiner is unsure if the applicant meant to say "propagation stage" or
   really means "prorogation stage". As the claims later refer to a "propagation
   stage", the examiner will assume the language of the claim is correct during
   the course of evaluating this application and wishes to draw the applicant's
   attention to this page and paragraph in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2, 4, 7, 8-10, 19, 21, 24, 26, 28, 34, and 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 2 recites the limitation "the size of the third bit sequence" in line 3. There is insufficient antecedent basis for this limitation in the claim.

2. Claim 4 recites the limitations "the first level" in line 2 and "the second level" in line 3. There are insufficient antecedent basis for these limitations in the claim.

3. Claims 7 and 8 recites the limitation "the expanded first bit sequence" in line 1-2. There is insufficient antecedent basis for this limitation in the claim.

4. Claim 9 and 10 recites the limitation "the third bit sequence" in line 1. There is insufficient antecedent basis for this limitation in the claim.

5. Claim 19 recites the limitation "the determination" in line 2. There is insufficient antecedent basis for this limitation in the claim.

6. Claim 21 recites the limitation "the two-level multiplexer" in line 1. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 24 recites the limitation "the size of the third bit sequence" in line 3. There is insufficient antecedent basis for this limitation in the claim.

8. Claim 26 recites the limitations "the first level" in line 2 and "the second level" in line 3. There are insufficient antecedent basis for these limitations in the claim.

9. Claim 28 recites the limitation "the expanded first bit sequence" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-12, 14-19, 22-25, 27, 28, 30-34, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964).

1. Claims 1 and 23: Kanda discloses a cryptographic engine as per claim 1 for performing cryptographic operations on a data block (col 1, lines 8-15). Kanda also discloses an integrated circuit layout associated with a cryptography engine as per claim 23 for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (col 1, lines 8-15). Kanda further discloses the cryptographic engine and the integrated circuit layout comprising:

a. A key scheduler configured to provide keys for cryptographic operation (col 7, lines 11-25).

b. Expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (col 15, lines 8-20 and Figure 8A-8D).

c. Permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (col 1, lines 31-46).

Kanda does not explicitly disclose:

a. A multiplexer circuitry having an input stage and an output stage, wherein the keys are provided at the input stage of the multiplexer circuitry.

b. Expansion logic coupled to the multiplexer circuitry.

c. Permutation logic coupled to the expansion logic.

However, Callum discloses:

a. A multiplexer circuitry having an input stage and an output stage (Figure 3, items 330, 28, and 64), wherein the keys are provided at the input stage of the multiplexer circuitry (Figure 3, items 330 and KR1-KR4).

  b. Expansion logic coupled to the multiplexer circuitry (Figure 3, items 330 and 319).

  c. Permutation logic coupled to the expansion logic (Figure 3, items 319 and 320).

One of ordinary skill in the art at the time the applicant's invention was made would have been motivated to employ Callum's teachings with Kanda because as Callum discloses, his teachings would allow a cryptography engine to better handle instruction-intensive bit permutation and thereby achieve greater cryptography speed (Callum's abstract).

2. Claims 2 and 24: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptographic engine, further comprising an Sbox configuration to alter a third bit sequence corresponding to the portion of the data block by compacting a size of the third bit sequence and altering the third bit sequence using Sbox logic (col 3, lines 31-52; col 10, last paragraph; and col 11, 1st paragraph).

3. Claims 3 and 25: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptography engine, wherein the cryptography engine is a DES engine (col 14, lines 15-28).

4. Claim 5: Kanda and Callum teach all subject matter as described in claim 1. Also, Kanda discloses the cryptography engine, wherein the first bit sequence is less than 32 bits (col 2, lines 1-21).

5. Claims 6 and 27: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptography engine, wherein the first bit sequence is four bits (col 17, lines 9-28).

6. Claim 7: Kanda and Callum teach all subject matter as described in claims 5. Also, Kanda discloses the cryptography engine, wherein an expanded first bit sequence is less than 48 bits (Figure 10).

7. Claims 8 and 28: Kanda and Callum teach all subject matter as described in claim 6. Also, Kanda discloses the cryptography engine, wherein an expanded first bit sequence is less than six bits (col 17, lines 9-28).

8. Claim 9: Kanda and Callum teach all subject matter as described in claim 7. Also, Kanda discloses the cryptography engine, wherein a third bit sequence is less than 48 bits (col 2, lines 22-39).

9. Claim 10: Kanda and Callum teach all subject matter as described in claim 8. Also, Kanda discloses the cryptography engine, wherein a third bit sequence is six bits (col 2, lines 22-39).

10. Claim 11: Kanda and Callum teach all subject matter as described in claim 9. Also, Kanda discloses the cryptography engine, wherein the second bit sequence is less than 32 bits (col 2, lines 1-21 and col 10, lines 22-35).

11. Claim 12: Kanda and Callum teach all subject matter as described in claim 10. Also, Kanda discloses the cryptography engine, wherein the second bit sequence is four bits (col 10, lines 22-35 and col 15, lines 20-53).

12. Claim 14: Kanda and Callum teach all subject matter as described in claim 1. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a plurality of stages (col 1, lines 18-67).

13. Claims 15 and 30: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a determination stage (col 15, lines 21-33).

14. Claims 16 and 31: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Callum discloses the cryptography engine, wherein the key scheduler comprises a shift stage (col 4, lines 46-67 and col 5, lines 1-5). Motivation for combining Kanda and Callum's teachings for claims 16 and 31 is the same as for claims 1 and 23.

15. Claims 17 and 32: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a propagation stage (col 2, lines 1-21).

16. Claims 18 and 33: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a consumption stage (col 3, lines 30-51).

17. Claims 19 and 34: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Callum discloses the cryptography engine, wherein a first shift amount for a first key is identified in the

determination stage using a first round counter value (col 4, lines 46-55 and

Figure 5). Motivation for combining Kanda and Callum's teachings for claims

19 and 34 is the same as for claims 1 and 23.

18. Claims 22 and 37: Kanda and Callum teach all subject matter as described in

claims 1 and 23 respectively. Also, Callum teaches the cryptography engine,

wherein the expansion logic and the permutation logic are associated with

DES operations (col 3, lines 32-47 and Fig 3, items 319 and 320). Motivation

for combining Kanda and Callum's teachings are the same as for claims 1

and 23 above.

Claims 4 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964) and Steinman et al

(U.S. 5,91,349).

1. Claims 4 and 26: Kanda and Callum teach all subject matter as described in

claims 1 and 23 respectively. They do not explicitly teach two 2-to-1

multiplexers on the first level coupled to two 2-to-1 multiplexers on a second

level. However, Steinman teaches 2-to-1 multiplexer usage (col 3 last

paragraph and col 4, 1st paragraph). It would have been obvious to one of

ordinary skill at the time the applicant's invention was made to employ

Steinman's teachings within the combination system of Kanda and Callum as

it would allow increased performance of a computer memory system by

reducing lost clock cycles (Steinman's abstract). It would have been obvious

to one of ordinary skill to have two 2-to-1 multiplexers on the first level

coupled to two 2-to-1 multiplexers on the second level because it would allow

for increased performance of DES or triple DES engine as the performance of

the computer improved in using 2-to-1 multiplexers. The speed up in clock

cycle improves the performance of DES.

Claims 13, 20-21, 29, and 35-36 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964) and

Windirsch (U.S. 6,760,439).

1. Claims 13 and 29: Kanda and Callum teach all subject matter as described in

    claims 1 and 23 respectively. They do not teach a cryptography engine,

    wherein the key scheduler performs pipelined key scheduling logic. However,

    Windirsch teaches pipelining being used in an encryption/decryption device

    (col 2, lines 12-35). One of ordinary skill would be motivated to incorporate

    Windirsch's teachings of pipelining into the combination system of Kanda and

    Callum as it would allow for simultaneous processing of a number of data

    streams as disclosed by Windirsch (col 2, lines 12-16).

2. Claims 20 and 35: Kanda and Callum teach all subject matter as described in

    claims 1 and 23 respectively. They do not teach a cryptography engine,

    wherein the multiplexer circuitry is a two-level multiplexer. However,

    Windirsch teaches a multiplexer circuitry being a two-level multiplexer (col 1,

    lines 35-47). One of ordinary skill would want to incorporate Windirsch's

    teachings into the combination system of Kanda and Callum as it would allow

for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, 1st paragraph).

3. Claims 21 and 36: Kanda and Callum teach all subject matter as described in claims 1 and 23 respectively. Also, Callum teaches the cryptography engine, wherein the multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer (col 3, lines 48-61; col 1, lines 39-46; and Fig 3). Windirsch teaches a two-level multiplexer (col 1, lines 35-47). The motivations for combining the teachings of Kanda, Callum, and Windirsch have already been mentioned.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. Buer (U.S. 5,671,284) discloses a data encryptor having a scalable clock.

2. Sugarhara et al (U.S. 2001/0011251) disclose an authentication engine coupled to a key generator.

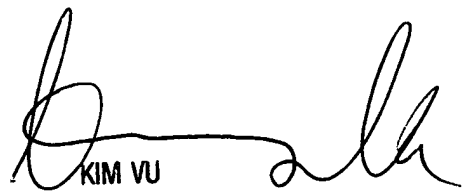3. Luyster (U.S. 6,578,150) discloses encryption using block cipher.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMIN
TECHNOLOGY CENTER 21